National Infrastructure Protection Center
CyberNotes

Issue #5-99 *March 3, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 12 and February 26, 1999. The table provides the operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Cobalt Networks, Inc[1].	Cobalt RaQ	The web server can read the shell history file of any user. Under certain circumstances this may expose passwords to unauthorized remote users.	Patch is available at: ftp://ftp.cobaltnet.com/pub/security	Cobalt RaQ shell history vulnerability	Medium	Bug discussed in newsgroups.
Computer Associates International Inc.[2]	ARCserve NT agents	The transfer of username and password between the ARCserve server and the client machine can be sniffed. Username is sent in the clear and the password is hidden with a simple XOR.	Updated files available at: http://support.cai.com/Download/patches	Username/ Password vulnerability in ARCserve	Medium/ High	Bug discussed in newsgroups and Web sites. The XOR value has also been provided in newsgroups.

[1] BUGTRAQ, February 25, 1999.
[2] BUGTRAQ, February 21, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Intel[3]	Pentium III	The identifying processor serial number contained on the Pentium III chip can be turned off and on without the user's knowledge.	Intel recommends that computer manufactures place on-off switch in the system BIOS.	Pentium III serial number track	**Special**	**Script to turn serial number on/off and track user has been demonstrated.**
Internet Security Systems, Inc[4]. (ISS)	Internet Scanner for Linux (trial version 5.3)	Local user can create a Denial-of-Service condition by placing certain files in the /tmp directory.	No workarounds or patches known at time of publishing.	ISS install.iss security hole	Low	Explanation of exploit available in newsgroups.
Irix[5] 6.2, 6.5.3 and other versions	Operating System (rpcbind)	Unauthorized remote user can insert and delete files by spoofing source address.	Filter 127.0.0.1 and local nets at border routers.	Rpcbind	Medium	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Kabsoftware[6]	Lydia	User password is stored in the file Lydia.ini. This file is usually found in C:\windows\lydia.ini. This file is encrypted.	No workarounds or patches known at time of publishing.	Lydia password file	Medium	Bug discussed in newsgroups and Web sites. Explanation of encryption and decrypting code posted to newsgroups and Web sites.
Linux[7]	Operating System (autofs)	Unauthorized user can potentially gain root access through a buffer overflow. At a minimum this overflow will cause kernel errors.	Various temporary solutions are available in newsgroup. The author has not presented his fix at time of publishing	Linux autofs buffer overflow	**High**	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Linux[8]	System Administration utility (Super)	Buffer overflow condition exists that will allow a local user to gain root access.	Patch located at: ftp://ftp.ucolick.org/pub/users/will/ To disable super you can execute the following as root. This will disable the setuid bit: Chmod 755 /usr/bin/super	Super local user buffer overflow	**High**	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Linux[9]	TetriNet daemon "Tetrix"	Buffer overflow condition exists that will allow an unauthorized user to execute code resulting in possible root compromise.	No workarounds or patches known at time of publishing. Post patches as of February 25, 1999 do not correct the problem.	Tetrix 1.13.16 buffer overflow	**High**	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.

[3] Reuters, Intel says probing alleged Pentium flaw, February 24, 1999.
[4] BUGTRAQ, February 20, 1999.
[5] BUGTRAQ, February 12, 1999.
[6] BUGTRAQ, February 19, 1999.
[7] BUGTRAQ, February 18, 1999.
[8] BUGTRAQ, February 26, 1999.
[9] BUGTRAQ, February 17, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Linux[10]	zgv	A privilege leaked to a child process can lead to a root compromise. The process is a processor privilege on Intel [iopl(3)], access to i/o ports.	A workaround is to disable the "-a" option.	Zgv privilege leak to child process	Medium (this attack currently requires a high degree of skill to obtain root access)	Bug discussed in newsgroups.
Linux[11] – Debian 3.9.6 to 3.11.6	System Administration utility (Super)	Two buffer overflow conditions exist that will allow an unauthorized user to gain root access.	Patch located at: ftp://ftp.ucolick.org/pub/users/will/	Debian Linux "Super" buffer overflow	**High**	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Linux[12] – Multiple	lsof Version 4.40 and prior	A buffer overflow condition exits that allows a local user to gain root access.	Patch available at: ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/patches/4.40/arg.c.patch	lsof buffer overflow	**High**	Bug discussed in newsgroups. **Numerous exploit scripts posted to newsgroups and Web sites.**
Linux[13] 2.0.34	Operating System (rpcbind)	Unauthorized remote user can insert and delete files by spoofing source address.	Filter 127.0.0.1 and local nets at border routers.	Rpcbind	Medium	Bug discussed in newsgroups.
Microsoft[14]	Internet Explorer (IE) 4	Information in the clipboard is not accessible to IE unless IE was the program that placed the information in the clipboard. A simple java script will allow IE to access data in the clipboard even if IE does not own the information.	Microsoft stated that a patch will be available with the next service pack release	IE4 vulnerability: The clipboard again	Low/ Medium	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
Microsoft Windows[15]	Explorer	If a user right clicks in explorer or attempts to delete a file longer than 217 characters, explorer will crash.	No workarounds or patches known at time of publishing.	Windows Explorer 217 character limitation	Low	Bug discussed in newsgroups and Web sites. Exploit script not required for the exploit.
Microsoft Windows[16] 95/98/NT	Windows Resource Kit (Taskpad)	Hostile Web site can run executables on the user's computer without the user's knowledge.	Patch is available at: ftp://ftp.microsoft.com/reskit	Taskpad Scripting Vulnerability	Medium/ High	Bug discussed in newsgroups and Web sites.

[10] BUGTRAQ, February 19, 1999.
[11] Debian GNU/Linux Security, February 15, 1999.
[12] HERT advisory # 002
[13] BUGTRAQ, February 12, 1999.
[14] BUGTRAQ, February 22, 1999.
[15] BUGTRAQ, February 13, 1999.
[16] Microsoft Security Bulletin, MS99-007.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows[17] 95, 98, and NT[18] **(change in risk level from CyberNotes #3-99 and #4-99)**	IIS and File Transfer Protocol (FTP)	Unauthorized remote user can log in (anonymous access included) and create a DoS condition. This may be a result of a stack overflow or bss (static pointers) overflow.	Patch available for various versions at: ftp://ftp.microsoft.com/bussys/iss	IIS DoS FTP	**High (**Military CERTs report this attack as resulting in system access.**)**	Explanation of exploit available in newsgroups. Exploit script has been published.
Microsoft Windows[19] NT[20]	Operating System (KnownDLL)	All users can read and write to the KnownDLLs list. A user can add malicious DLLs with the same name as system DLLs to gain higher privileges or execute other actions. Vulnerability is restricted to machines that the malicious user is interactively logged onto.	Microsoft is currently working on a patch. Strong protection is possible if the following is add to the registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManger: Name: ProtectionMode Type: REG_DWORD Value: 1	Windows NOT KnownDLL List Vulnerability	Medium	Bug discussed in newsgroups and Web sites.
NcFTP[21]	NcFTPd	An unauthorized remote user can execute arbitrary code. The extent of the possible compromise is limited by the program's character restriction. Further exploitation may be possible but has not been verified.	Patch available at: http://www.ncftp.com/download Vendor reports that only one byte may be changed with this overflow	NcFTPd limited buffer overflow	Low	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
NFR[22]	Network Flight Recorder (NFR) 2.0.2-Research	Unauthorized user can gain root access.	Patch available from the NFR web site at: http://www.nfr.com	Stack overflow in NFR Web Server	**High**	Bug discussed in newsgroups and Web sites.
Seattle Lab[23]	SLMail 3.1 or 3.2 with Remote Administration Service enabled	SLMail allows changes to mail services using HTTP protocol over TCP port 180. An unauthorized user can change mail accounts and services. Other attacks are possible.	Remote administration should be disabled if possible. Other workarounds have been posted but their effectiveness has not been completely tested.	SLMail service change over port 180	Medium	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.
SmartMax[24]	Mail-Max SMTP server for Windows	Buffer overflow condition exists that will allow an unauthorized user to execute code resulting in root compromise.	No workarounds or patches known at time of publishing.	Mail-Max remote buffer overflow	**High**	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites.

[17] eEye Digitial Security Team, Advisory Code - IISE01.
[18] BUGTRAQ, January 25, 1999.
[19] L0pht Security Advisory, February 18, 1999.
[20] Microsoft Security Bulletin, MS99-006.
[21] Proof of Concept Security Advisory, February 23, 1999.
[22] Network Associates, Inc., Security Advisory, February 16, 1999.
[23] NTBUGTRAQ, February 25, 1999.
[24] BUGTRAQ, February 14, 1999.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun Solaris[25] 2.6	Operating System (rpcbind)	Unauthorized remote user can insert and delete files by spoofing source address.	Filter 127.0.0.1 and local nets at border routers.	Rpcbind	Medium/ High	Bug discussed in newsgroups. Exploit script posted to newsgroups and Web sites. **Hackers known to be using this attack.**
Trend Micro[26]	InterScan VirusWall for Solaris	HTML request with two "GET" commands combined in the same request will result in the second file not being checked for viruses. Both Netscape Communicator and Microsoft Internet Explorer are known to formulate these types of requests during normal use.	**Vendor stated that they originally unable to recreate this problem.** Patch posted at: http://www.antivirus.com	InterScan Viruswall second file failure	Medium	Normal browser use may result in virus infection.
Triactive[27]	Remote Management Software	If Basic authentication is used, the username and password for remote machines is stored in HKLM\SOFTWARE\TriActive\Remote Manger\Username.	Vendor recommends that users opt for the Challenge and Response authentication	Triactive's remote manger software plaintext password	Low/ Medium (high priority targets for hackers)	Bug discussed in newsgroups and Web sites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - Any vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[25] BUGTRAQ, February 12, 1999.
[26] Backhats Security Advisory, February 22, 1999.
[27] BUGTRAQ, February 19, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between February 12 and February 26, 1999, listed by date of script, script name, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 65 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
Feb 26, 1999	**SDI-super.c**	**Exploit code for buffer overflow vulnerability that exists in the "super" program. See Debian Linux "Super" buffer overflow in "Bugs, Holes & Patches" above.**	
Feb 25, 1999	Qwcrash.pl	Denial-of-Service program designed to disrupt quakeworld servers.	
Feb 25, 1999	pbomb.pl	Program that attempt to cause a Denial-of-Service condition by opening multiple connections to a given machine.	
Feb 25, 1999	Novell_login	Fake login screen for Novell that captures usernames and passwords in a file called os31337.sys.	
Feb 25, 1999	**netdog.c**	**General hacker tool that includes scanner, IRC nukes, mailbomber and other tools.**	
Feb 24, 1999	**RAT**	**Remote administration tool similar to but less powerful than Back Orifice.**	
Feb 24, 1999	**blackhole.c**	**A small backdoor program.**	
Feb 23, 1999	**9x_c1sco.zip**	**Program that claims to kill all Cisco 7XX routers running IOS/700 v4.1(x).**	
Feb 23, 1999	9x_logn.zip	A logind Trojan horse.	
Feb 23, 1999	Gammaprog 1.50	Bruteforce password cracker for web based e-mail systems and Post Office Protocol (POP) 3 servers.	
Feb 23, 1999	icmpush22.tgz	Program that gathers information on a remote system by sending ICMP error packages.	
Feb 23, 1999	ie4.clipboard	Exploit code that allows remote attacker to view user's clipboard.	
Feb 23, 1999	**Net-RawIP v0.06**	**Perl module that manipulates raw Internet Protocol (IP) packets and Ethernet headers. The version is ported to Perl 5.005 and BSD, and includes the oshare script (causes Microsoft Windows 98 machines to lock).**	
Feb 22, 1999	**SDI-lsof.c**	**Exploit code for the lsof buffer overflow vulnerability.**	
Feb 22, 1999	Arcserve.nt.agents.txt	Explanation and exploit code for the ARCserver NT agents username and password vulnerability.	
Feb 22, 1999	Gammaink.zip	Graphic Front-end for the Gammaprog bruteforce password cracker.	
Feb 22, 1999	iss.exploit.c	Exploit code for the tmp-symlink problem in Internet Security Scanner (ISS) that can be used for Denial-of-Service or root compromise.	
Feb 22, 1999	**lsof-xploit.c**	**Exploit code for the lsof buffer overflow.**	
Feb 22, 1999	Nmap.tcl	Script that facilitates Port scanning of IRC users.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
Feb 22, 1999	Sm4ck.c	Program that claims to add three backdoors on machines that it is executed on (operating system not specified).	
Feb 21, 1999	**Humpdee2.tgz**	**Improved version of exploit for the Linux rpc.mountd vulnerability.**	
Feb 21, 1999	Imapx.c	Remote exploit for Linux imap vulnerability.	
Feb 20, 1999	Bncx.c	Exploit for Linux BNC.	
Feb 20, 1999	Humpdee.tgz	Exploit for Linux rpc.mountd vulnerability.	
Feb 20, 1999	vcu10.exe	A suite of password cracking utilities.	
Feb 20, 1999	Windows98.pingflood	Exploit code for Windows 98 pingflood Denial-of Service vulnerability.	
Feb 19, 1999	ADMsnmp.0.1.tgz	Tool for remote data gathering, brute force cracking and remote command execution.	
Feb 19, 1999	ADM-spoof-NEW.tgz	Packet spoofing program that includes Send/Spoof IP, GGP Echo packets, connection resetting, and SYN flood.	
Feb 19, 1999	**cgiscan2.c**	**Scanner that checks for various common vulnerabilities in CGI scripts.**	
Feb 19, 1999	jester.tgz	Backdoor server and spoofer.	
Feb 19, 1999	**NetBusPro v2.0**	**Trojan horse program with a Graphical User Interface (GUI), proxy support, file manager, web-cam capture, registry manager, hosts scheduler, application redirect, chat and many other features.**	
Feb 19, 1999	Net-RawIP v0.05e.tar.gz	Perl module that manipulates raw Internet Protocol (IP) packets and Ethernet headers. The version is ported to Perl 5.005 and BSD, and includes the oshare script (causes Microsoft Windows 98 machines to lock).	
Feb 19, 1999	NT 4.0 DLL hack	Explanation and exploit script for NT 4.0 DLL cache permissions.	
Feb 19, 1999	Qps.gz	QPOP/UCB/SCO scanner.	
Feb 19, 1999	server.c	Backdoor server.	
Feb 19, 1999	xtvscreen.suse6	Program that can be used to overwrite files on SuSE6.	
Feb 18, 1999	ctontab-backdoor.sh	Shell script that binds a root shell to a selected port for a specific amount of time (crontab controlled).	
Feb 18, 1999	junk.tar.gz	Exploit scripts for the mail.local security hole.	
Feb 18, 1999	listerine.tar.gz	Script that tests for the NcFTPd security hole.	
Feb 18, 1999	mailfrm.tar.gz	Exploit scripts for the mail.local security hole.	
Feb 18, 1999	nbtscan.zip	Automates the running of "nbtstat –A" on a set of IP addresses.	
Feb 18, 1999	**Net-RawIP v0.05d**	**See description above**	
Feb 18, 1999	Netscape.window.spoof	Explanation and exploit scripts of the Netscape communicator window spoofing bug using HTML and JavaScript.	
Feb 18, 1999	nfr.sof	Explanation and exploit scripts that allows a remote user to gain system management privileges of a Network Flight Recorder v2.0.2 in default configuration.	
Feb 18, 1999	**Nmap-2.08.tgz**	**Network-scanning tool that has a variety of scanning modes, including stealth, Xmas, and Null stealth. This release adds more operating system fingerprinting and several bug fixes. Note: This tool continues to be used by hackers. A number of systems become unstable when scanned if patches are not applied.**	
Feb 18, 1999	tcplogd.0.0.tar.gz	Stealth-scan detector.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
Feb 18, 1999	Topdesk.passwd	Description of decryption technique for TOPdesk.	
Feb 18, 1999	vpr11.zip	Unix password cracker for use on Microsoft Windows machines.	
Feb 17, 1999	**lsof**	**Exploit program for the lsof vulnerability. See lsof buffer overflow in "Bugs, Holes & Patches" above.**	
Feb 17, 1999	Websitepro	Exploit program that allows remote user to replace files on some websites.	
Feb 16, 1999	**Cain v1.0**	**Password utility that recovers Windows 95/98 passwords including logon, Share, screen savers, dial-up and link passwords.**	
Feb 16, 1999	inetd.DoS.c	Denial-of-Service program that exploits the inetd buffer overflow.	
Feb 15, 1999	defunct.cpp	Program that attempts to circumvent security measures by translating IP address to raw addresses (identifier). Overrides restrictions set by proxies.	
Feb 15, 1999	**exscan-0.4.tar.gz**	**Port scanner with a strobe scanning capability.**	
Feb 15, 1999	mailmaxbof.c	Exploit code for the Mial-Max SMTP server buffer overflow.	
Feb 15, 1999	Thetaprog.tgz	Bruteforce password cracker for Hotmail password reminder.	
Feb 15, 1999	tracerouteflood.c	Exploit code that will allow any user to use traceroute as a UDP or ICMP flooder.	
Feb 12, 1999	ActiveX.file.system.object	Exploit code that uses the FileSystemObject vulnerability to modify files on an Active Server Page (ASP) web server.	
Feb 12, 1999	dsu_sat	Exploit code that causes a binary overflow resulting in a terminated DSU satellite communication.	
Feb 12, 1999	Fakebo.bof.c	Exploit code that uses a buffer overflow in fakebo to execute code that results in root access.	
Feb 12, 1999	NT.explorer.DoS	Exploit code for Windows NT explorer long filename vulnerability.	
Feb 12, 1999	s10scan.pl	Port scanning code that adds address of false machines in an effort to mislead logging programs.	
Feb 12, 1999	sbounce.pl	Perl coded program that functions as an IRC bounce.	
Feb 12, 1999	Serve-U.DoS	Exploit code for Serve-U FTP software that results in a Denial-of-Service condition.	
Feb 12, 1999	Ultraprog.zip	Brute force cracker for the MailCity password reminder.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period remain the same those trends two weeks ago.

1. Several hackers/hacker groups appear to be using coordinated scans and probes from different sites.
2. Large numbers of scans and attacks continue to be directed at machines running the Linux operating system.
3. Scanning for Internet Message Access Protocol (IMAP) and POP continues.
4. Significant increase in reports of NetBus and Back Orifice scanning.
5. Significant increase in the number of scans directed specifically against Domain Name Servers.
6. Viruses are now being written to capture and transmit information.

Viruses

A list of the top ten viruses infecting two or more sites as reported to various anti-virus vendors has been categorized into the two tables below. The first table list macro viruses, and the second table lists other viruses. Macro viruses have, historically, spread fastest due to their ability to be transferred by e-mail.

For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite), trends (based on number of infections during the last three months reported), and approximate date first found.

Note: Virus reporting is normally 6 to 8 weeks behind the first discovery of infection. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages, as updates become available.

The viruses listed in the virus table have infected over 510 sites in January, which is a slight increase in the number of reported infections from the last prevalence table. The number 1 ranked virus for January/February accounted for 36 infected sites, and the last virus listed in the tables infected 19 sites. A total of 467 distinct viruses were reported this month, infecting over 2,000 sites.

Table 1 – Macro viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date
1	CAP	Macro	Steady	April 1997
2	Class	Macro	Increasing	September 1998
3	ColdApe	Macro	Increasing	December 1998
4	Laroux	Macro	Increasing	July 1997
5	Temple	Macro	Increasing	December 1998
6	Npad	Macro	Steady	December 1996
7	Concept	Macro	Decreasing	December 1996
8	Hark	Macro	Decreasing	December 1998
9	Munch	Macro	Increasing	October 1998
10	Wazzu	Macro	Steady	December 1996

Table 2 – Other viruses:

Ranking	Common Virus Name	Type of Virus	Trends	Date
1	One_half	Multi	Steady	October 1995
2	Form	Boot	Steady	September 1991
3	Junkie	Multi	Steady	July 1994
4	W95/CIH	File	Increasing	July 1998
5	AntiCMOS	Boot	Steady	October 1995
6	Parity_Boot	Boot	Steady	September 1993
7	AntiEXE	Boot	Decreasing	September 1994
8	Ripper	Boot	Steady	March 1994
9	Empire.Monkey	Boot	Steady	July 1994
10	DelCMOS.B	Boot	Increasing	January 1999

Seagate Backup Exec Warning - Users of Seagate Backup Exec software should be aware that the virus data file downloaded between January 23rd and February 9th contains an incorrect virus signature. This virus data file will cause all Visual Basic class files to be identified as containing a virus. Normal operation of the Network Associates VirusScan API as integrated with Seagate's Backup Exec is to first attempt to clean an infected file. If the file(s) can not be cleaned prior to backup they are deleted from the system.